

[Utah Code Ann. §§ 13-44-101 to -301](#)

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
YES	Most expedient time possible and without unreasonable delay	NO

More Details

Scope of this Summary	Notification requirements applicable to persons that own, license or maintain covered info. Some types of businesses may be exempt from some or all of these requirements and non-commercial entities may be subject to different requirements.
Covered Info	First name or first initial and last name, plus: Social Security number; driver's license or state identification card number; or financial account, credit card or debit card number in combination with any required security or access code or password that would permit access to a resident's financial account.
Form of Covered Info	Electronic Only
Encryption Safe Harbor	Statute does not apply to information that is encrypted or protected by another method that renders the data unreadable or unusable.
Breach Defined	Unauthorized acquisition that compromises the security, confidentiality or integrity of the covered info, excluding certain good faith acquisitions by employees or agents.
Consumer Notice	<p><u>Timing</u>: Must be made in the most expedient time possible without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.</p> <p><u>Method</u>: By written notice sent by first-class mail to the most recent known address, telephone notice, electronic notice (if it is the primary method of communication with resident or is consistent with E-SIGN), or publishing notice in a newspaper of general circulation in a manner consistent with Utah's public notice statute.</p>
Delayed Notice	Notification may be delayed if law enforcement determines notice may impede a criminal investigation.
Harm Threshold	Notification not required if, after reasonable and prompt investigation, the covered entity determines that identity theft or fraud has not occurred and is not reasonably likely to occur.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify them immediately following discovery of a breach if misuse of covered info has, or is reasonably likely to, occur. Must cooperate by sharing info relevant to the breach with the data owner.
Potential Penalties	Violations may result in civil penalties.

Last revised on March 26, 2018

This summary is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. Additional requirements or conditions may apply to any or all provisions referenced herein. For more information about the state data breach notification laws or other data security matters, please seek the advice of counsel.